



(19)

Europäisches Patentamt
Europäischer Patentamt
Office européen des brevets



(11)

EP 0 893 759 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.01.1999 Bulletin 1999/04

(51) Int Cl. 6: G06F 9/46, G06F 17/30,
H04L 29/06

(21) Application number: 98305686.2

(22) Date of filing: 16.07.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 21.07.1997 GB 9715256

(71) Applicant: XEROX CORPORATION
Rochester, New York 14644 (US)

(72) Inventors:

- Eldridge, Marge
Gt. Shelford, Cambridge, CB2 5AH (GB)
- Flynn, Michael
Cambridge, CB2 2RN (GB)

- Jones, Chris
Cambridge, CB1 2LG (GB)
- Kleyn, Michael
Blackheath, London SE3 (GB)
- Lamming, Michael
Cambridge, CB2 2RN (GB)
- Pendlebury, David
Cambridge, CB1 2LG (GB)

(74) Representative: Reynolds, Julian David
Rank Xerox Ltd
Patent Department
Parkway
Marlow Buckinghamshire SL7 1YL (GB)

(54) Token-based document transactions

(57) A system including any number workstations, file servers, printers and other fixed devices coupled in a network, and a number of portable devices carried by users and coupled to the network by infrared (IR) link. Each portable device emulates its user's personal satchel for documents: the device is programmed to receive transmit and store document or service tokens (tokens). Preferably, the token comprises a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service. The tokens are distributed from one person to another by transmission of IR data packets, and once a network-connected computer, printer or multifunction device has received a token via IR transceiver associated with it, a search request can be derived from the token and document references (e.g. WWW URLs) satisfying the token can be obtained via a search engine. For each URL obtained, the corresponding electronic document can be retrieved from a repository and displayed or printed. The portable device

is preferably a handheld or wristwatch computer with a graphical display for enabling the user to transfer tokens, and the fixed devices preferably include a scanner/copier/printer having its own IR transceiver.

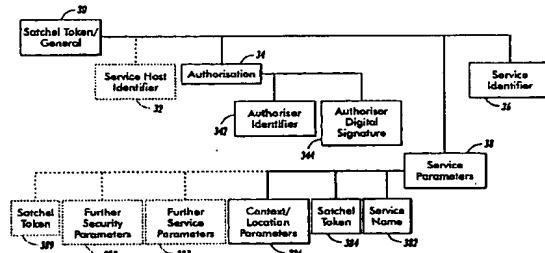


FIG. 3A

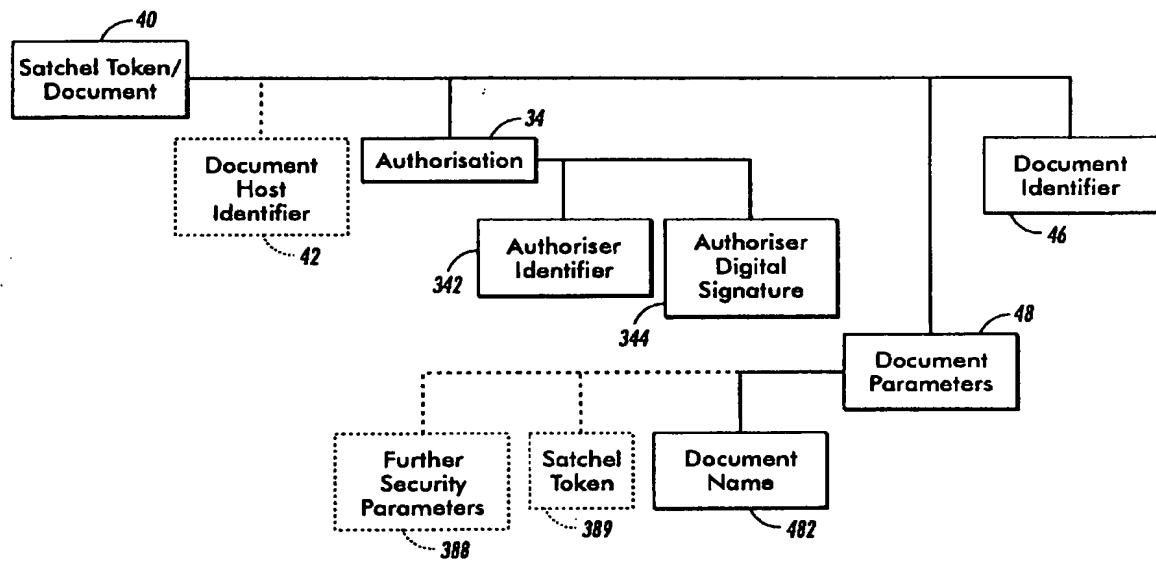


FIG. 3B

Description

The present invention relates to data processing, and more particularly relates to the transfer between computing devices, and the retrieval by such devices, of document related information. Even more particularly, the invention concerns such information retrieval, transfer and processing using tokens.

While the use of portable computing devices is becoming more widespread, it is as yet not possible to store in such devices the electronic files for all the documents that a user may wish to have access to (e.g. due to storage capacity limitations), and the transfer of bulk documents between such devices, or between one such device and a desktop office or home computer may be time consuming or otherwise user unfriendly. At the same time, there is growth in the provision of electronic document repositories and expanding use of document transfer via the internet.

This situation is addressed in EP-A-691,619 (hereafter "EP'619"), which discloses a system including any number workstations, file servers, printers and other fixed devices (including multifunction devices) coupled in a network, and a number of portable devices (e.g. handheld or wristwatch computer) carried by users and coupled to the network by infrared (IR) link. Each portable device emulates its user's personal satchel for documents: the device is programmed to receive transmit and store document references (World Wide Web URLs), each of which is associated with an electronic document stored in an electronic repository at a site on the web. Documents are distributed from one person to another by transmission of document URLs, and a document is sent to a printer by beaming that document's URL to an IR transceiver associated with that printer. Mobile workers away from their offices can make use of such a system in order to perform activities dealing with electronic and paper documents. These activities include printing, scanning, viewing, presenting, requesting, giving and distributing documents, and accessing document services.

A problem is that users of documents who are mobile, (i.e. away from their office, at remote sites of their own company, at sites of other companies, at hotels, etc.) have a need to perform various activities related to electronic and paper documents. These activities include sharing documents with others they meet, printing out or faxing their documents, acquiring documents from others, acquiring documents by scanning, having processing performed by services on their documents (e.g. format conversion, OCR of scanned documents, language translation). They further have a need to do so quickly and easily with minimum disruption to ongoing higher level activities.

Small personal devices which can perform computation such as mobile phones, pagers, and personal digital assistants are increasingly being carried by mobile workers all the time. Wireless data communication tech-

nologies for these devices are becoming widely available (e.g. infrared, short-range radio, and cellular phone radio). However, these modes of communication lack the necessary bandwidth for the general movement of

5 electronic documents because such documents can be lengthy, complex, rich in images and hence have large data sizes. Systems which make use of fixed link communication can handle such large data loads quickly but they are difficult to connect to at remote sites. This may
10 be for both physical reasons (wrong kind of connector, no ethernet tap nearby) and for security reasons (no login account available at remote site within the same company, no IP address, or connecting to local network at an other company is prohibited). In order for personal
15 devices for mobile users to be easy to carry everywhere, they must be small. Hence their ability to carry data and power is limited.

Current approaches to supporting mobile users' document needs usually involves either relying on a human assistant that can always be reached, taking a full computer (e.g. a laptop) or collecting and distributing paper or floppy disks from a briefcase.

It would be desirable to have systems and methods which support these activities and enable transfer documents between people and devices in a manner which is simple, quick, and secure. These techniques must work within the technology constraints prescribed by small limited-power portable devices.

The present invention provides a method carried
30 out in a data processing device including a processor, memory, and a user interface, comprising: (a) receiving at least one user input, the user input(s) defining at least one token component, the token components defining a document related entity and a property of the entity,
35 the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related, and (b) compiling a token, the token including
40 the component(s) received in step (a).

Preferably, prior to step (b), step (a) is repeated a plurality of times.

The data processing device may comprise a portable computing device, and step (a) comprises receiving
50 user inputs via touchscreen or a keyboard.

The data processing device may comprise a fixed computing device, and step (a) comprises receiving user inputs via touchscreen, a keyboard, and/or mouse.

The present invention further provides a method
55 carried out in a data processing device including a processor, memory, and a user interface, comprising: (d) receiving a first user input designating a graphical object corresponding to a stored token, the token comprising

a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service, (e) receiving a second user input indicating that the token is to be sent to another data processing device, (f) encoding the token in a data packet, and (g) transmitting the data packet.

The present invention further provides a method carried out in a data processing device including a processor, memory, and a user interface, comprising: (h) receiving a data packet (i) decoding the data packet to derive a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service, and (j) storing the token derived in step (i).

The present invention further provides a method carried out in a data processing device including a processor, memory, and a user interface, the data processing device being couple in a network to one or more other data processing devices, at least one of the data processing devices including means for storing a repository of electronic documents, comprising: (k) receiving at least one user input designating a token, the token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service, (l) decoding the token to determine therefrom one or more document references, the or each document reference corresponding to a document within said repository satisfying said feature constraint.

Preferably, step (k) comprises the previously mentioned method.

The method may further comprise the step of: (m)

displaying the or each document reference determined in step (l).

The method may further comprise the step of (n) in response to a second user input designating one of the displayed document references, retrieving the document corresponding to said document reference from said repository and, optionally, displaying said document or a portion thereof.

The method may further comprise the step of: (o) in response to a third user input, causing the document corresponding to said document reference to be printed.

The present invention further provides a data processing device when suitably programmed for carrying out the method of any of the preceding claims, the device comprising a processor, a memory, and a user interface.

The present invention further provides a data processing device comprising: a processor, a memory coupled to the processor, and a user interface coupled to the processor and to the memory and adapted to be operable by a user to generate user inputs, means for receiving at least one user input, the user input(s) defining at least one token components, the token components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related, and for compiling a token, the token including the received token components.

The present invention further provides a system for accessing or distributing electronic documents, including: a repository of electronic documents, each document having a corresponding document reference, and a plurality of objects, at least one of said objects being portable or mobile, each object including means for communicating with the or each other object and with a user interface, and means for receiving, storing and/or transmitting a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service.

The present invention further provides a portable device for accessing or distributing electronic documents, including: means for communicating with fixed

or mobile electronic devices and with a user interface, at least one of said devices including means storing a repository of electronic documents, each document having a corresponding document reference, and means for receiving, storing and/or transmitting a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service.

The present invention further provides an apparatus for scanning, copying and/or printing documents, including: means for accessing a repository of electronic documents, each electronic document having a corresponding document reference, means for communicating with one or more of a plurality of objects, at least one of said objects being portable or mobile, and with a user interface, and means for receiving, storing and/or transmitting a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service.

The invention employs "Satchel Document Tokens" - a special form of reference to a document or to a document service in portable devices, systems and methods for supporting mobile worker's document activities. These Satchel Document Tokens are henceforth simply referred to as "tokens".

In accordance with the invention, tokens can be stored in small personal portable electronic devices and can be transmitted between holders of such devices. They can also be transmitted to appropriately equipped document devices (printers, scanners, copiers, faxes). Tokens contain the information necessary to access documents, to invoke a document services with appropriate parameter settings, or to initiate the actions of a document device with appropriate parameter settings. In addition, the token contains the security information which provides safeguards to ensure that unauthorised use of the documents or document services that are referenced in the token is precluded.

In preferred embodiments, a token contains at least the following components.

Basic Operation. The token specifies the particular operation that is to be performed, e.g. getting the document or performing a service (printing, scanning, faxing, converting). The action may be identified very generically here, with parameter settings used to identify the exact operation more specifically.

Address of document or document service. The token contains the information necessary to find the document or service. The address could consist of the network address of a server and the file path name of a document. A WWW Uniform Resource Locator (URL) is an example of a document address, and is used in the current Satchel prototype.

Parameters. The token contains a set of parameter settings that may be needed by subsequent services that are triggered by transmitting the token to a device. Parameters are used to further specify the document or document service (e.g. Number of copies to print). Some parameters may themselves be tokens. The specific types parameters required depends on the particular service.

Visible Name. The token contains a string or icon which can be displayed to identify the document or service to which the token refers for the benefit of the user.

Security Information. The security component of a token contains information to support ensuring that only the intended use of the token is possible.

The security information includes a digital signature of the information in the token. The digital signature is a digest of information in the token and its encryption with the document owner's private key. This follows well known prior cryptographic art relating to public/private key cryptography (see US-A-4,405,829). These signatures can only be generated by the personal portable device since only it has the private key. The signature ensures the integrity of the token and attests that the token did originate from a known portable device.

The security information can also include specified conditions that will restrict access to a document. For example, it may include (1) an expiry date beyond which access to the document is no longer granted, (2) the condition that a payment or certificate for release must be associated with the token, and/or (3) a requirement that only a given device be used to print the document.

The security information can include a recipient's public key or name to indicate that the returned document be encrypted with the given public key or the known public key associated with the recipient's name. This ensures that only the intended recipient of the document can make use of the returned document and that an intercepted copy of either the encrypted document or the token is of no use to anyone other than the intended recipient.

More generally, information for supporting fees and usage rights such as can be expressed in more complex fees and usage rights languages (such as described in Stelik, M., "Letting Loose the Light: Igniting Commerce in Electronic Publication. In *Internet Dreams: Arche-*

types, Myths, and Metaphors. Edited by Mark Stefik. MIT Press, 1996), may be associated with the token.

Tokens which include security information are presented to "secure documents servers". A secure server contains a "gatekeeper" which verifies signatures on tokens and examines the specified conditions associated with the token and then acts accordingly (e.g. encrypting the document with the appropriate key). The public key for verifying the signature is obtained through a parameter in the security information which identifies the owner of the document or from a server which stores users' public keys.

The problems mentioned in the opening part of this disclosure are overcome by using computing devices, systems and methods employing a token based approach, as discussed in further detail herein.

There are set out below numerous disadvantages of conventional technology, together with details of how the token-based techniques provides advantageous solutions.

(i) A laptop is too heavy to carry everywhere all the time. Tokens can fit into smaller amount of memory which will require less power, allowing the device to be even smaller. The smaller a device, the more easily it can be carried everywhere.

(ii) Unanticipated need: If the user has forgotten to take the paper document or electronic document, he or she cannot give the document. A Satchel user can always provide a token for a document. There is no longer the burden of having to remember which documents to take.

(iii) Speed: A wireless transfer of a token between devices will always require less communication time than a wireless transfer of the actual document. This streamlines and speeds up the transfer transaction and improves its reliability. The lower transmission power requirements contribute to keeping the device small.

(iv) Remote login is awkward: When using a laptop, the user attempts to find a means to login remotely to his/her home office machine or server to access documents. This is awkward and complicated, the physical connection devices may be wrong, access to the local network may be barred (no local login), or dial-up to home office may be expensive and slow. This is alleviated by providing the security information component in the token.

(v) Transferring an electronic document from one user to another is awkward, since the users must have a medium (floppy disks, which may be too small) or laptop-laptop network which will be clumsy to set up. Also, with tokens, any associated processing (e.g. format conversion) of a document can be performed when the token is submitted ("cashed-in") and anywhere where applications for processing are available.

(vi) Dynamic documents: A token can contain a ref-

erence to a document whose contents change (e.g. a weather forecast). The user can thus give a token for "the latest version" of a document. This is not possible with a static copy of the document from paper, laptop or floppy.

(vii) Security improvement: The loss or theft of the device doesn't mean documents are immediately accessible, only tokens. The secure server can be instructed to no longer honour tokens from the device (analogous to revoking a credit card). In the case of using a laptop or floppy, either the data is stolen, or the user must ensure all data on the laptop is encrypted.

10 A further benefit is in the enablement of diverse document-related activities, examples of which are given below.

15 (i) Tradable services. By encapsulating services in tokens, they can be passed on and distributed just like document tokens.

20 (ii) Partially Specified Services: The service may only be partially specified in the token. A simple example of a partially specified document service is one which prints a given document in a particular way on a printer (e.g. duplex two-up). The remaining specification of the service (e.g. the actual printer, the number of copies) may not yet be specified, but the token can nonetheless be passed from one user to another. The recipient can then use it as a known, reliable, and easy way of having a specific service performed, with their choice of further options.

25 (iii) Network supplied processing: The burden is on the token-enabled servers on the network to get the desired action performed, not on the limited personal device. By using tokens, neither the data nor the application of the document need be locally present, either on the portable device itself or at any local server. Service execution and invoking applications for particular data formats can be performed where the appropriate software is available.

30 Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

35 Figure 1 illustrates schematically a portion of the network infrastructure which may be used to implement embodiments of the invention;

40 Figure 2 shows a portable computing device used in accordance with an embodiment of the invention; Figure 3 illustrates schematically the components of a token used in accordance with an embodiment of the invention, (a) in general form, and (b) the document form;

45 Figure 4 is a schematic flow chart of the steps in exchanging tokens in accordance with an embodi-

ment of the invention;

Figure 5 is a schematic diagram of the steps involved in the transfer, in accordance with an embodiment of the invention, of a token between a portable computing device and one or more fixed devices;

Figure 6 is an illustration of the steps involved, in accordance with an embodiment of the invention, in decoding the token of Fig. 3, once received; and Figure 7 is a schematic flow chart of the steps involved in carrying out the appropriate action as specified in the token as received as in Fig. 6.

1. System hardware

It will be appreciated that the present invention may be implemented using conventional computer network technology, either using a local area network (LAN) or, more suitably, a wide area network (WAN). The invention has been implemented using conventional web browser software (e.g. Netscape) providing cross-platform communication and document transfer over the internet. However, it will be appreciated that the invention may be implemented using different system configurations: see EP'619. It will be appreciated that each fixed machine forming part of the network may be a PC running Windows™, a Mac running MacOS, or a minicomputer running UNIX, which are well known in the art, or any suitable processor-controlled network computer. For example, the PC hardware configuration is discussed in detail in *The Art of Electronics*, 2nd Edn, Ch. 10, P. Horowitz and W. Hill, Cambridge University Press, 1989.

As is known, upon request of a user at a first machine, a document stored on a second machine may be retrieved and sent from the second machine over the internet, via any number of intermediate machines to the first machine. Also, the document may be retrieved using as a unique identifier its World Wide Web URL, as discussed in EP'619 and international application WO-

A-_____, based on British patent application 9708175.6 (agent's ref. R/97005). Preferably also connected to the network are any number of processor-controlled printers, scanners, fax machines or multifunction devices (capable of scanning, printing, copying and/or faxing, etc.) (not shown), as discussed in EP'619. Multifunction devices are discussed in more detail in EP-A-741,487. Each machine coupled to the network is also equipped with appropriate hardware and software, which is known in the art, for communication with portable computing devices, such as personal digital assistants (PDAs), handheld PCs, or pocket or wristwatch computers.

A variant of the infrastructure described in the aforementioned patent applications, for implementing the present invention, is shown in Fig. 1. The pervasive computer network 21 has, as is known, an infrared transceiver 22 for each room, desk, workstation, copier,

printer etc., coupled thereto. (For the sake of clarity, only one transceiver 22 is illustrated). In addition, however, the network 21 is coupled to the conventional telephone network 24 by means of gateway 26, which is known in the art. In this way, the portable computing device 2 is able to communicate with devices on the network 21 not only by IR signals to/from transceivers 22, but also (when additionally or alternatively provided with digital radio frequency communications hardware (not shown))

- 5 by RF signals to/from a digital cellular base station 28 of the telephone network 24. Suitably, the RF communications hardware (not shown) complies with the GSM digital standard, thereby permitting transmission of digital data between the portable device 2 and the base station 28, which suitably comprises a GSM receiver/transmitter.
- 10
- 15

A preferred form of portable computing device is shown in Fig. 2. This device 2 is discussed in more detail in EP'619. However, it will be appreciated that the computing device may be fabricated in a multitude of forms:

- 20 for example, the device 2 may be of any of the forms disclosed in European patent application EP-A-_____ (attorney's reference D/95594/JDR), corresponding to U.S. application S.N.
- 25

- 28 _____ ("Personal storage device for application and data transfer", filed 28 March 1996). In its preferred form, each portable computing device 2, and each of the fixed machines on the network, is equipped for infrared communication and suitably, the data packets transmitted between the computing device 2 and the fixed machines, and enabling the document(s) to be retrieved, conform to the physical and link layer formats (IrLAP) described in the industry standard Infrared Data Association (IrDA) specification, version 1.0, which is well known in the art.
- 30
- 35

The tokens concept described here provides an essential component of a system solution that addresses these needs of the mobile worker (e.g. Satchel; EP'619), within the technological constraints described above.

A token contains the small amount of essential information which allows the system (token-capable server software resident on public networks and private networks) to initiate actions which produce the desired result.

- 40
 - 45
 - 50
 - 55
- For example, printing out a document only needs a simple interaction: The document's token is selected on the user interface of the small device. This token is incorporated as a parameter of a token identifying the print service. When the latter token is received by the server software via a wireless and then a wired connection (e.g. an infrared receiver which is tethered to the local network), the servers acts on the receipt of the token and causes the document to be retrieved, processed, and printed. In this way it is only the token that is transmitted from the personal portable device via wireless means and then it is fixed, wired, communications that is then used to move the actual document data, appropriately processed, to the end device (a printer

in this example). The net effect is that a user can produce a desired action in a quick and simple way.

2. Satchel Token Components ("packet encoding")

Figures 3(a) and 3(b) are schematic diagrams of the contents of a Satchel Token. They show, abstractly, the main components of a Satchel Token. Figure 3(a) is the more general form which specifies the structure of any token, whether it is for a service or for a document. Figure 3(b) is a simpler version of the same token - one which specifies the form of a Satchel Token when the token only embodies a straight document request.

In Figs. 3(a) and 3(b) and the following description, text in bold indicates a component which may have further components (e.g. Service Parameters). Boxes and lines which are dashed indicate components which may be present in some tokens, but need not be present in all tokens, i.e. they are not required in order to make a valid Satchel Token.

Referring to Fig. 3(a), the components (32, 34, 342, 344, 36, 38, 382-389) of the general form of the satchel token 30 are schematically illustrated.

All the components (32, 34, 342, 344, 36, 38, 382-389) taken together form a **Satchel Token** general 30. They are stored inside a user's PDA 2 (but they can also be stored in user's personal computers/workstations) as small packets having the structure indicated in Fig. 3. They are taken out of this form and linearised (made into a straight linear sequence of ASCII characters) when needed. This can be done for two reasons: (i) so that a token can be transported through some communications medium (wired or wireless) and (ii) so that the token as a whole can be taken as a linear sequence of ASCII characters for secure hashing and then digital signing operations to form the token's digital signature component.

The general token 30 includes a Service Host Identifier 32 which identifies a host machine on a network. This component indicates to the system where the document or service is available from a host machine on the network. Typically this is in the form of a standard Internet Fully Qualified Domain Name.

The Service Host Identifier 32 need not be filled into the token 30 by the user's PDA 2. This flexibility is essential in order to implement the context sensitive capabilities feature of the Satchel System. This component 32 of a token 30 may be filled in at a later stage in the processing of a token 30. For example, the infra-red transceiver device which accepts and conveys tokens can fill in the Service Host Identifier 32 - in order to specify a Service Host Identifier 32 that is appropriate for that transceiver device's location.

Authorisation - The general token 30 includes a component 34 which in turn contains the two main security components. It provides the means by which the system can verify that the token is genuine and has not been tampered with.

The first security component is an Authoriser Identifier 342 - This component indicates the person that created the token 30. The Authorisation identifier 342 may be as simple as an ASCII string of the user's name, or

- 5 be as complex as a full X.509 identity certificate (see ITU-T Recommendation X.509 - CCITT document "The Directory-Authentication Framework"). The second security component is an Authoriser Digital Signature 344, which is a string created by the following method: (a)
- 10 linearise all other components in the token to produce an ASCII string, (b) produce a hash of the string using any suitable well-known secure hash function (e.g. MD5, SHA; see *Applied Cryptography* by Bruce Schneier, 1996, John Wiley and Sons), and (c) encrypt the hash with the user's private key, which is only kept in the PDA. Note that the Authoriser Digital Signature 344 itself is not part of the hash, but the Authoriser Identifier 342 is.

Another component of the general token 30 is the Service Identifier 36. The Service Identifier 36 is a component which identifies the particular service (or document) that is to be invoked (or requested) on behalf of the user. A feature of the system according to the invention is that this Service Identifier 36 may only identify a general class of service, with the actual service being 20 invoked being deduced by the system from this Service Identifier 36 and the additional Service Parameters (discussed below) provided.

- 25 All the components (32, 34, 342, 344, 36, 38, 382-389) taken together form a **Satchel Token** general 30. They are stored inside a user's PDA 2 (but they can also be stored in user's personal computers/workstations) as small packets having the structure indicated in Fig. 3. They are taken out of this form and linearised (made into a straight linear sequence of ASCII characters) when needed. This can be done for two reasons: (i) so that a token can be transported through some communications medium (wired or wireless) and (ii) so that the token as a whole can be taken as a linear sequence of ASCII characters for secure hashing and then digital signing operations to form the token's digital signature component.
- 30 The general token 30 includes a further component designated Service Parameters 38. This component itself has several components 382-389 which serve to further specify the service request. The Service Parameters 38 includes Service Name 382, which identifies how a service is identified to the user as a visible name in the user interface of the PDA 2. This may be simply a familiar name, e.g. "Print" or "Scan" or "Fax", a graphic icon, or can be more complex, e.g. a type-in form to be filled in by the user. Also included in Services Parameters 38 is Satchel Token 384. A Satchel Token 30 can itself contain zero or more further **Satchel Tokens** 384, 389. This is a key aspect of the design of this invention in that it allows more complex user requests to be created in the form of Satchel Tokens 30 which are composed of other Satchel Tokens 384, 389. This is indicated in Fig. 3 by the Satchel Token boxes 384, 389. They 35 can contain another full token, be it a General Satchel Token 30 or simple Document Satchel Token 40.
- 40 The general token 30 includes a component 36 which identifies the service or document to be performed. This component 36 may be a simple name, e.g. "Print", or it may be a more complex type-in form to be filled in by the user. The component 36 may also include parameters which identify the context in which the service or document is to be performed. These parameters may be filled into the token 30 either by the PDA device 2 itself or the wireless transceiver devices (infra-red). The location parameters 386 can include, for example: the type of document device (printer, scanner, fax) that the transceiver is attached to, the local name of the document device, the room in which the request was made, the time when the request was made, the country in which the request was made.

The Service Parameters 38 further includes Context/Location Parameters 386. This component contains parameters which identify the context in which the request is made. The parameters may be filled into the token 30 either by the PDA device 2 itself or the wireless transceiver devices (infra-red). The location parameters 386 can include, for example: the type of document device (printer, scanner, fax) that the transceiver is attached to, the local name of the document device, the room in which the request was made, the time when the request was made, the country in which the request was made.

As shown, as part of the Service Parameters 38, Further Service Parameters 387 may be included. This component contains parameters which can specify the particulars of a request even further. Examples of Further Service Parameters 387 include: the number of copies to be printed, the phone number of a fax machine that a document is to be faxed to, the name of a scanned document. In addition, another component of the Service Parameters 38 may be Further Security Parameters 388. The use of the token 30 can be restricted, and these restrictions supported, by indications in the Further Security Parameters component 388. Such additional information can include: a cryptographic key to use to encrypt a document when the token is used to request it, an expiry date for the validity of the token, a restriction on the type or identity of the device that the document can be printed on. Additionally, a full specification of the digital property rights of the document can be added using a statement in a digital property rights language (DPRL) (see the abovementioned M. Stefik reference). Since tokens 30 can contain tokens, security restrictions that must be satisfied can be associated with tokens at each level.

Referring now to Fig. 3(b), this is a simplification of Fig. 3(a), and shows the simpler form of token - a **Satchel Token/Document** (or "Document Token") 40 - when the token is simply a request to access a document. In Figs. 3(a) and 3(b) like reference numerals denote like elements.

In the case of the token 40 of Fig. 3(b), the component embodying the Service Identifier 36 is Document Identifier 46. This indicates to the system where the document is located. Also, the component embodying the Service Host Identifier 32 is the Document Host Identifier 42.

Also, for the document token 40, a component designated Document Parameters 48 is included. This component itself has several components which serve to further specify the document request. The Document Parameters 48 includes a Document Name component 482, indicating how the document is named for visible display in the PDA user interface - i.e. a title, as well as satchel token 389 and Further Security Parameters as in Fig. 3(a).

3. Transactions with tokens

Figure 4 is a schematic flow chart of the steps in exchanging a token (between the PDAs of users A and B), in accordance with an embodiment of the invention. Initially (step s1) an input is received from user A, requesting the transmission of a token. This request may be input by user A via the user interface of the PDA by means of button presses, selection from pull down menus, and/or dragging and dropping of icons, as is well known in the art (see, e.g. EP '619).

In response to the user request, the PDA of user A (hereafter PDA A) transmits (step s2) a query (by wire-

less, and preferably IR, signals) for the context of user A, i.e. for the identification of the users (here: B) of those PDAs which are in range of communication. Next, the PDA of user B (hereafter PDA B) receives the context request query and prepares a response (step s3). Once compiled in suitable form, the "Service available" reply is sent (step s4) by PDA B. This amounts to saying that it is OK to send the token from user A's PDA to that of user B. When sending this reply, PDA B can provide a user identity or cryptographic key (public) associated with the "Service Available" information.

Once the "Service Available" indication is received by PDA A, user A is prompted to make a further selection (step s5) via the user interface of PDA A, corresponding to the action "Beam Token to User B" - see EP '619). Then, at step s6, the necessary components (see Fig. 3) are assembled and the token (30, 40) constructed. This is followed by the wireless transmission of the token (i.e. as an IR data packet) (step s7) from PDA A to PDA B. Once received (step s8) at PDA B, the newly-arrived token is stored in PDA B (step s9) in the conventional manner, and this may be with or without further intervention by user B to place (an icon for) the newly-received token in an appropriate directory.

Figure 5 is a schematic diagram of the steps involved in the transfer, in accordance with an embodiment of the invention of a (print service) token between a portable computing device (PDA) and a fixed device (printer) in order to accomplish the printing of a document. The top part of Fig. 5 is the same as Fig. 4, except that PDA B is replaced by an IR transceiver 22 on the network 21 of Fig. 1: the transceiver 22 may be physically attached to (and electronically coupled to) or embedded in, the printer on which it intended to print the document. Also, steps s1' to s8' in Fig. 5 correspond to the steps s1 to s8 of Fig. 4, except that the service is a "Print Document" service, and the token transmitted is a Satchel Print Service token. Parameters (see Fig. 3) corresponding to the specific action to perform, in this case printing, may be incorporated into the token either by the PDA 2 when assembling the token (s6, s6') or by the transceiver 22 upon receipt, depending on the circumstances.

In Fig. 5, step s8' is followed by the step (s10) of adding parameters to the received satchel/print service) token: these may include any of the (components of the) parameters 38, 48 of Fig. 3. Once the parameters have been appended to the token, the token is sent over the network to workstation 50.

At workstation 50, upon receiving the token, the first step (s11) is to decode the token: this involves checking the Authorisation (see Fig. 3), and is described in more detail below in connection with Fig. 6. Then, the token is analysed at step s13: the substeps constituting the procedure of step s13 are described in more detail below with reference to Fig. 7. An element of this routine is the request for a document held in an electronic repository - here it is illustrated as being stored on a re-

mote file server 52 (which may be in a different building or in a different country), although it will be appreciated that the document could be stored locally on the workstation 50.

Thus, in order to request the document the document token is sent (step s14) to file server 52 where it is decoded (step s15) upon receipt, so as to extract the Document Identifier 46 (see Fig. 3(b)), e.g. a WWW URL. Using the Document Identifier 46, the document data (electronic file) are retrieved by the file server 52. The document data are then sent over the network at step s17, in the conventional manner, to the workstation 50 which originally received the Print Service token.

Once the document data are received at the workstation 50, a check is made to see whether the data must be converted (to a different format), and if so, the conversion is carried out at step s18. For example, printer 54 associated with transceiver 22 may be capable of printing only in Postscript® format; and step s10 therefore included adding parameters to the token designating that the data file sent ultimately to the printer must be converted to Postscript® format. Following conversion (if necessary), the (converted) document data are sent (step s19) to the printer 54. Upon receiving the document data, the document is printed (s20) by the printer in the conventional manner.

Figure 6 shows in detail the substeps of the decode Satchel token step of Fig. 5. First the linear ASCII string form of the token as received at workstation 50 is re-created in its structured form, as shown in Fig. 3. Then, a test is made at step s124 to see if the Authorisation Digital Signature (344; Fig. 3) verifies. If the test is failed, an "Authorisation verification failure" message is returned (step s126), i.e. output to the user in a conventional manner.

If success is obtained in the test of step s124, the action (service) - here printing a document - is invoked by the workstation 50, as described elsewhere.

Figure 7 shows in detail the substeps involved in the Analyse Token step in Fig. 5. Initially, the print service is invoked (step s131), by virtue of the Service Identifier parameter 36 (Fig. 3) designating a print request. Then, the Service Parameters 38 (Fig. 3) are examined (step s132); for example, the printing device which is to perform the print (service) may have been specified by user (and included as a parameter) prior to transmitting the token, or may have been added (step S10; Fig. 5) based on context/location parameters 386 (Fig. 3(a)). The token may include further service parameters, as discussed in Section 2 above. This enables the exact print service required (e.g. printer id, number of copies, 2-sided, etc.) to be deduced (step s133).

Once this has been done, the document to be printed is requested (step s134), and the document token sent to the file server (see Fig. 5). Then, the capabilities of the chosen printer are examined (step s135); this may show that the printer can only print with a certain paper size, with only certain fonts, or only documents in Post-

script® format, for example. In this way, the conversion techniques which need to be performed on the document data received from the file server (52; Fig. 5) can be determined (step s136). Then, once the document data are sent (s17) to the workstation 50 (Fig. 5), the necessary conversion can be carried out (step s18) prior to despatch of the document to the chosen printer.

10 Claims

1. A method carried out in a data processing device including a processor, memory, and a user interface, comprising:

(a) receiving at least one user input, the user input(s) defining at least one token component, the token components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related, and
 (b) compiling a token, the token including the component(s) received in step (a).

2. A method carried out in a data processing device including a processor, memory, and a user interface, comprising:

(d) receiving a first user input designating a graphical object corresponding to a stored token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service,
 (e) receiving a second user input indicating that the token is to be sent to another data processing device,
 (f) encoding the token in a data packet, and
 (g) transmitting the data packet.

3. A method carried out in a data processing device including a processor, memory, and a user interface, comprising:
- (h) receiving a data packet
 (i) decoding the data packet to derive a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service, and
 (j) storing the token derived in step (i).
4. A method carried out in a data processing device including a processor, memory, and a user interface, the data processing device being coupled in a network to one or more other data processing devices, at least one of the data processing devices including means for storing a repository of electronic documents, comprising:
- (k) receiving at least one user input designating a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service,
 (l) decoding the token to determine therefrom one or more document references, the or each document reference corresponding to a document within said repository satisfying said feature constraint.
5. A data processing device when suitably programmed for carrying out the method of any of the preceding claims, the device comprising a processor, a memory, and a user interface.
6. A data processing device comprising:
- a processor,
 a memory coupled to the processor, and
 a user interface coupled to the processor and to the memory and adapted to be operable by a user to generate user inputs,
 means for receiving at least one user input, the user input(s) defining at least one token components, the token components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service, and for compiling a token, the token including the received token components.
7. A system for accessing or distributing electronic documents, including: a repository of electronic documents, each document having a corresponding document reference, and a plurality of objects, at least one of said objects being portable or mobile, each object including means for communicating with the or each other object and with a user interface, and means for receiving, storing and/or transmitting a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service.
8. A portable device for accessing or distributing electronic documents, including: means for communicating with fixed or mobile electronic devices and with a user interface, at least one of said devices including means storing a repository of electronic documents, each document having a corresponding document reference, and means for receiving, storing and/or transmitting a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic ad-

dress of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service.

9. An apparatus for scanning, copying and/or printing documents, including: means for accessing a repository of electronic documents, each electronic document having a corresponding document reference, means for communicating with one or more of a plurality of objects, at least one of said objects being portable or mobile, and with a user interface, and means for receiving, storing and/or transmitting a token, the token comprising a plurality of components defining a document related entity and a property of the entity, the token components including an operation component designating a document related operation, an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service.

5

10

15

20

25

30

35

40

45

50

55

12

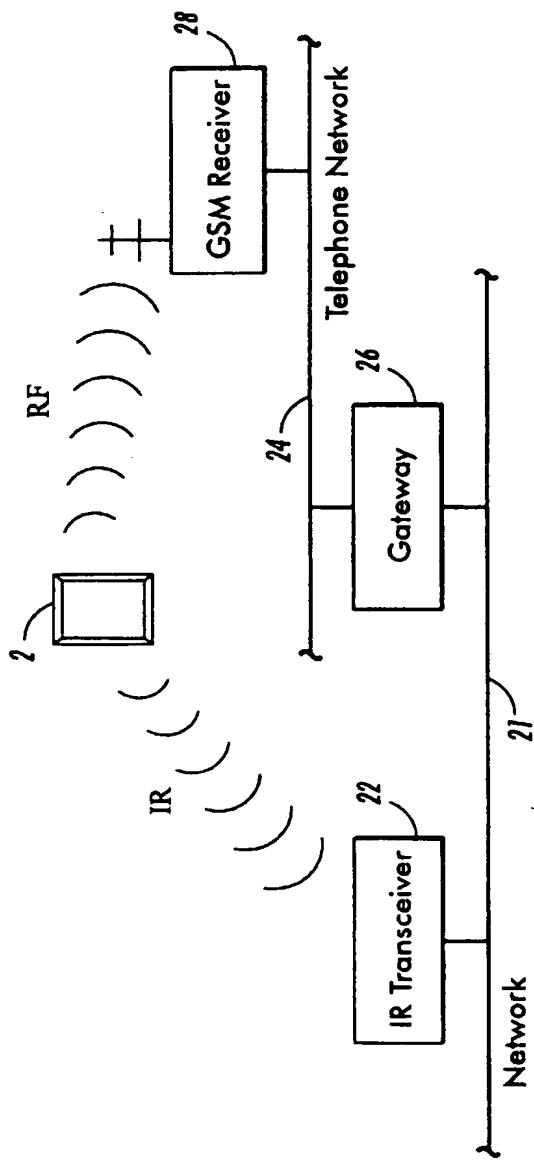


FIG. 1

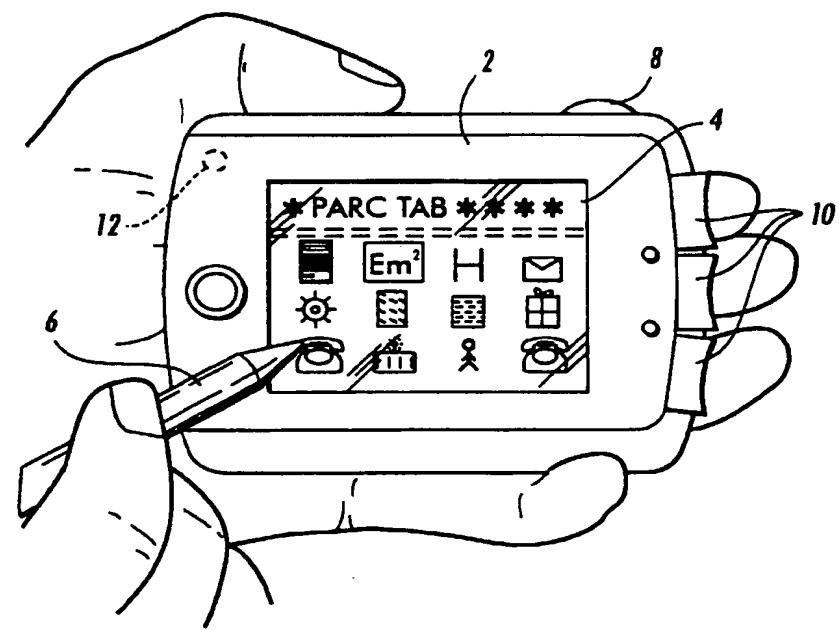


FIG. 2

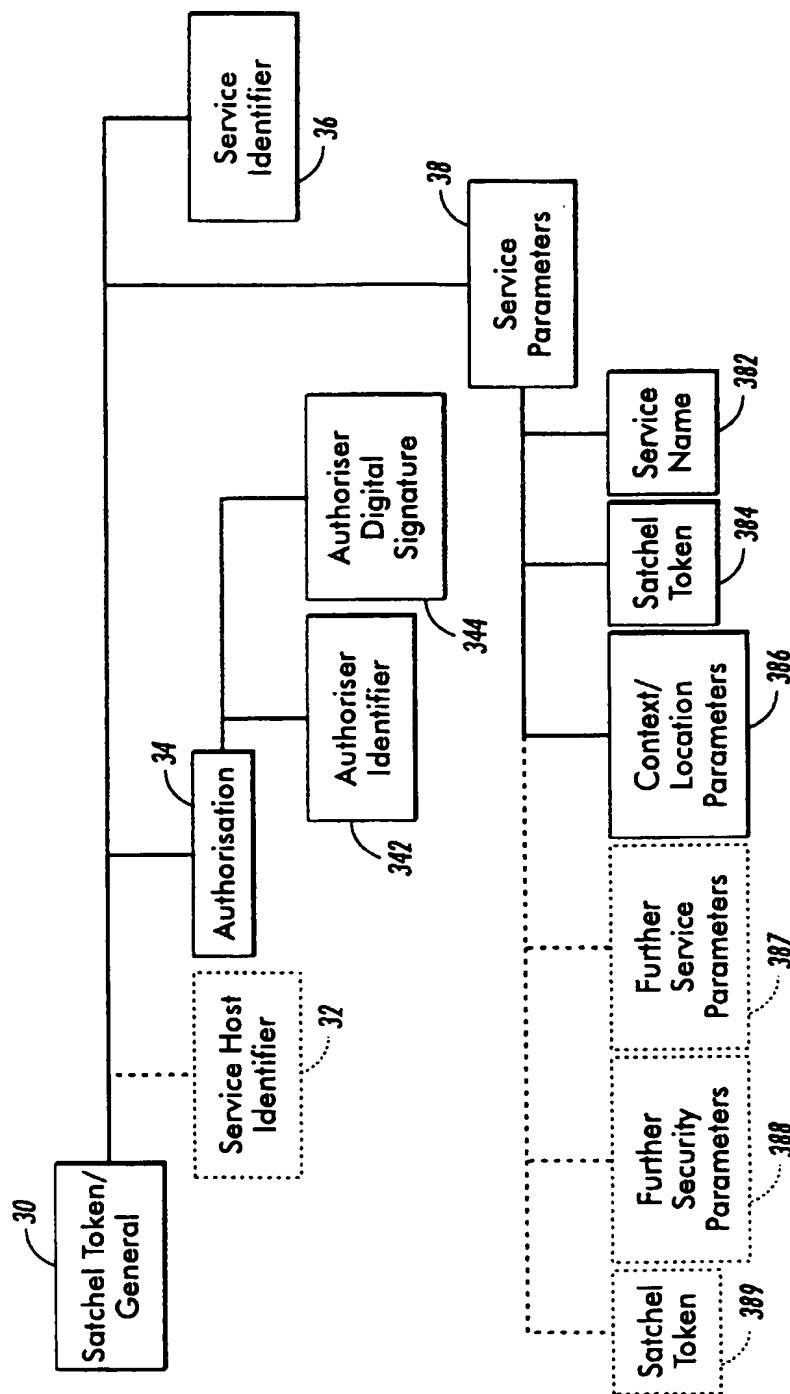


FIG. 3A

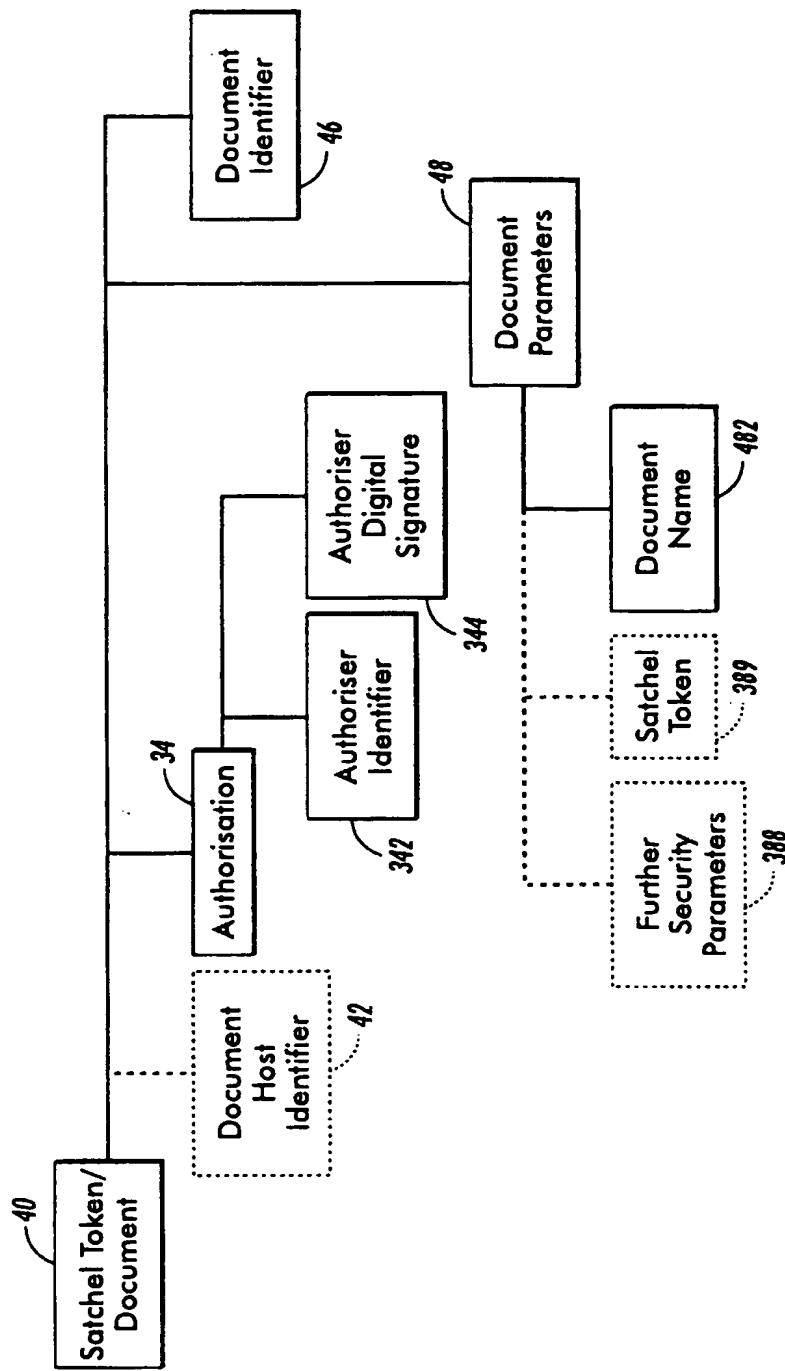


FIG. 3B

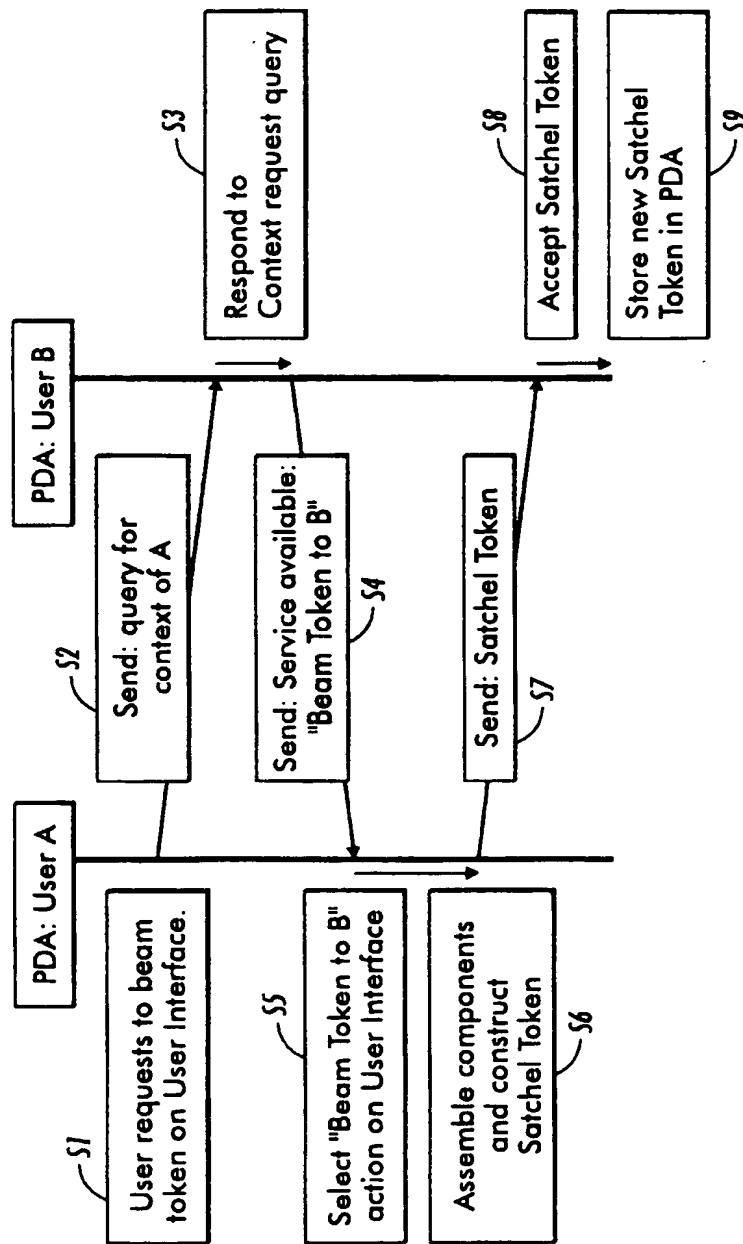


FIG. 4

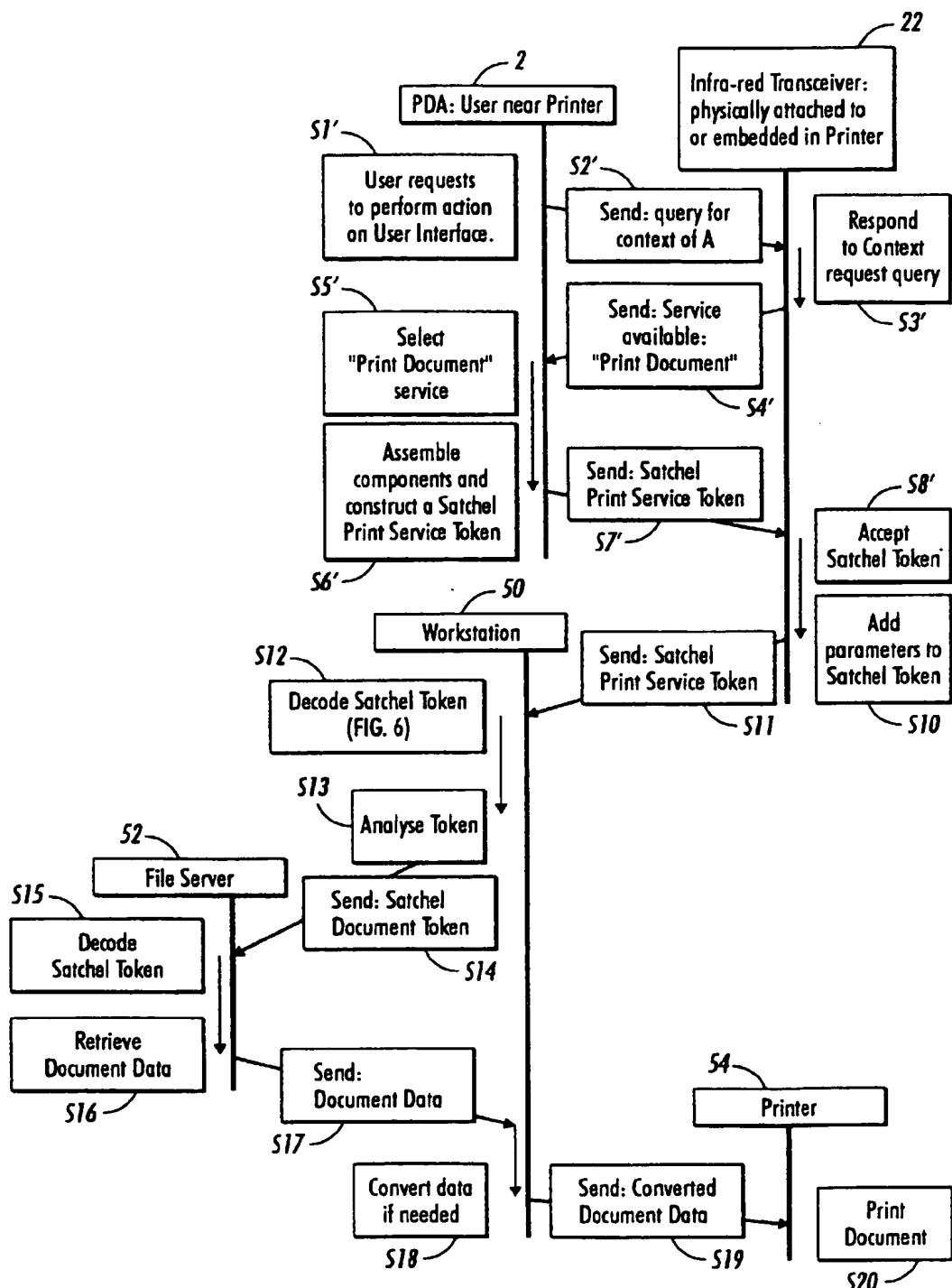


FIG. 5

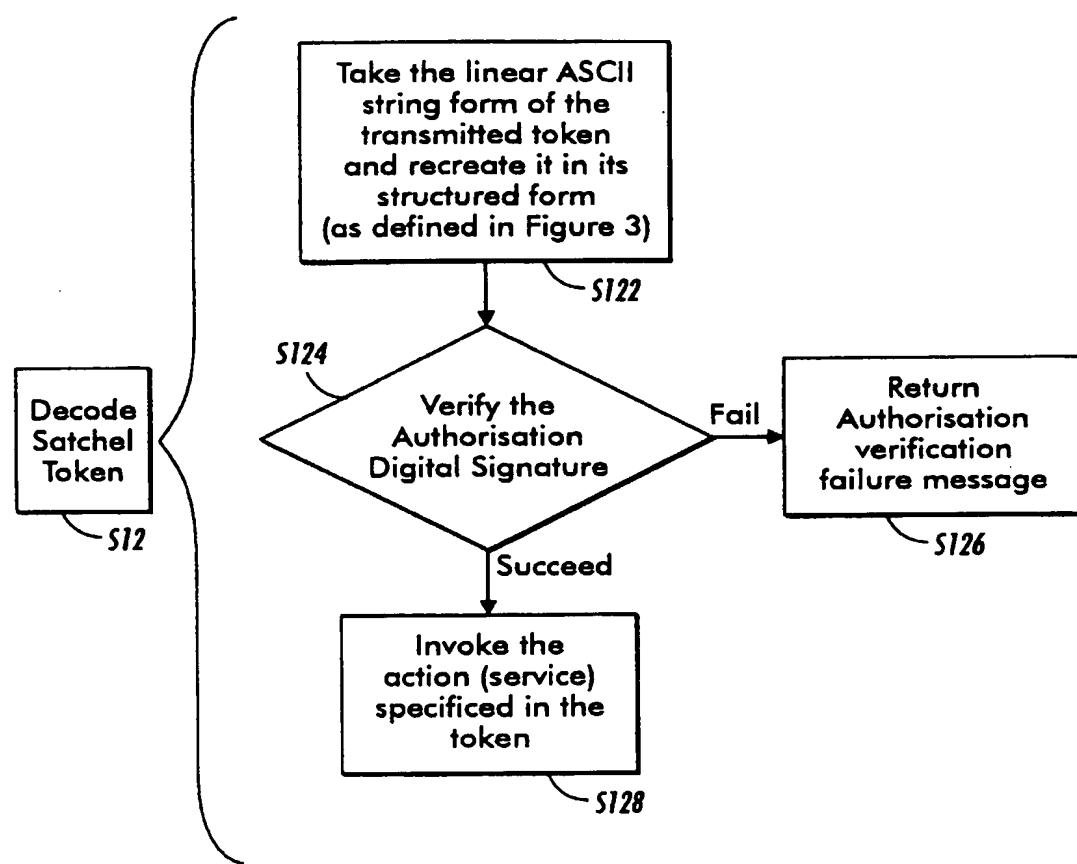


FIG. 6

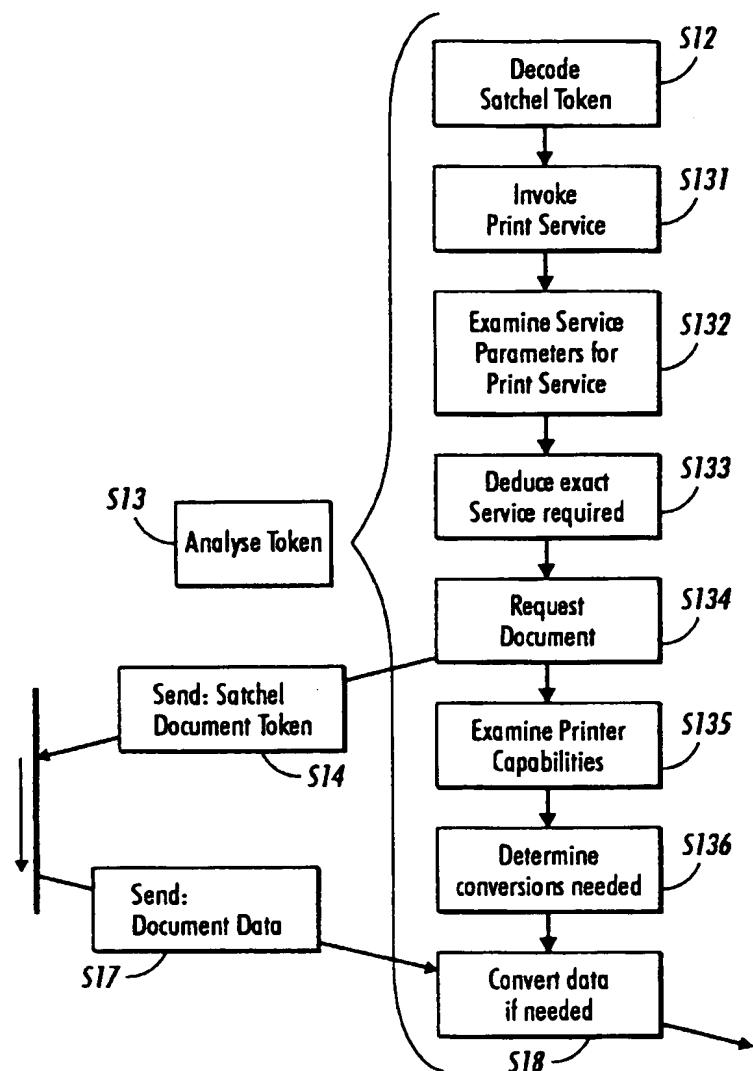


FIG. 7